Question 1

What characteristic describes spyware?

- a network device that filters access and traffic coming into a network
- **software that is installed on a user device and collects information about the user**
- an attack that slows or crashes a device or network service
- the use of stolen credentials to access private data

Question 2

Which two devices would be described as intermediary devices? (Choose two.)

- **wireless LAN controller**
- server
- assembly line robots
- **IPS**
- gaming console
- retail scanner

Question 3

Which statement describes network security?

- It supports growth over time in accordance with approved network design procedures.
- It synchronizes traffic flows using timestamps.
- **It ensures sensitive corporate data is available for authorized users.**
- It prioritizes data flows in order to give priority to delay-sensitive traffic.

Question 4

What is a characteristic of a switch virtual interface (SVI)?

- **An SVI is created in software and requires a configured IP address and a subnet mask in order to provide remote access to the switch.**

- Although it is a virtual interface, it needs to have physical hardware on the device associated with it.
- SVIs do not require the no shutdown command to become enabled.
- SVIs come preconfigured on Cisco switches.

Explanation: Cisco IOS Layer 2 switches have physical ports for devices to connect. These ports do not support Layer 3 IP addresses. Therefore, switches have one or more switch virtual interfaces (SVIs). These are virtual interfaces because there is no physical hardware on the device associated with it. An SVI is created in software.
The virtual interface lets you remotely manage a switch over a network using IPv4 and IPv6. Each switch comes with one SVI appearing in the default configuration "out-of-the-box." The default SVI is interface VLAN1.

Question 5

What is a user trying to determine when issuing a ping 10.1.1.1 command on a PC?

- if the TCP/IP stack is functioning on the PC without putting traffic on the wire
- **if there is connectivity with the destination device**
- the path that traffic will take to reach the destination
- what type of device is at the destination

Explanation: The ping destination command can be used to test connectivity.

Question 6

Refer to the exhibit. An administrator is trying to configure the switch but receives the error message that is displayed in the exhibit. What is the problem?

```
Switch1> config t
         ^
% Invalid input detected at '^' marker.
```

ITExamAnswers.net

- The entire command, configure terminal, must be used.
- The administrator is already in global configuration mode.

- **The administrator must first enter privileged EXEC mode before issuing the command.**
- The administrator must connect via the console port to access global configuration mode.

Explanation: In order to enter global configuration mode, the command configure terminal, or a shortened version such as config t, must be entered from privileged EXEC mode. In this scenario the administrator is in user EXEC mode, as indicated by the > symbol after the hostname. The administrator would need to use the enable command to move into privileged EXEC mode before entering the configure terminal command.

Question 7

Match the descriptions to the terms.

the part of the operating system that interfaces with applications and the user	shell
users interact with the operating system by typing commands	CLI
enables the user to interact with the operating system by pointing and clicking	GUI
the part of the OS that interacts directly with the device hardware	kernel

Explanation: A GUI, or graphical user interface, allows the user to interact with the operating system by pointing and clicking at elements on the screen. A CLI, or command-line interface, requires users to type commands at a prompt in order to interact with the OS. The shell is the part of the operating system that is closest to the user. The kernel is the part of the operating system that interfaces with the hardware.

Question 8

Which two OSI model layers have the same functionality as two layers of the TCP/IP model? (Choose two.)

- Session
- **Transport**
- **Network**

- Data link
- Physical

Explanation: The OSI transport layer is functionally equivalent to the TCP/IP transport layer, and the OSI network layer is equivalent to the TCP/IP Internet layer. The OSI data link and physical layers together are equivalent to the TCP/IP network access layer. The OSI session layer (with the presentation layer) is included within the TCP/IP application layer.

Question 9

Which PDU is processed when a host computer is de-encapsulating a message at the transport layer of the TCP/IP model?

- bits
- frame
- packet
- **segment**

Explanation: At the transport layer, a host computer will de-encapsulate a segment to reassemble data to an acceptable format by the application layer protocol of the TCP/IP model.

Question 10

Which three layers of the OSI model provide similar network services to those provided by the application layer of the TCP/IP model? (Choose three.)

- physical layer
- **session layer**
- transport layer
- **application layer**
- **presentation layer**
- data link layer

Explanation: The three upper layers of the OSI model, the session, presentation, and application layers, provide application services similar to those provided by the TCP/IP model application layer. Lower layers of the OSI model are more concerned with data flow.

Question 11

What OSI physical layer term describes the measure of the transfer of bits across a medium over a given period of time?

- **throughput**
- bandwidth
- latency
- goodput

Question 12

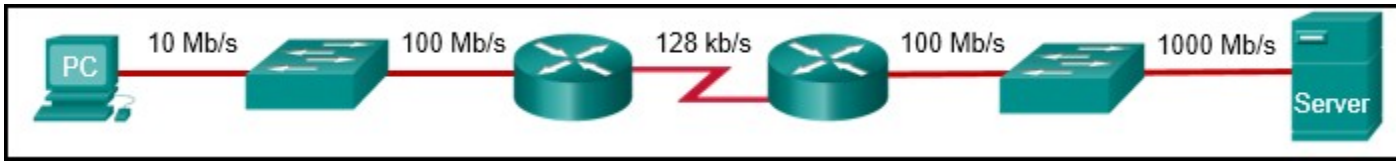
Which two statements describe the characteristics of fiber-optic cabling? (Choose two.)

- **Fiber-optic cabling does not conduct electricity.**
- Fiber-optic cabling has high signal loss.
- **Fiber-optic cabling is primarily used as backbone cabling.**
- Multimode fiber-optic cabling carries signals from multiple sending devices.
- Fiber-optic cabling uses LEDs for single-mode cables and laser technology for multimode cables.

Explanation: Fiber-optic cabling is primarily used for high-traffic backbone cabling and does not conduct electricity. Multimode fiber uses LEDs for signaling and single-mode fiber uses laser technology. FIber-optic cabling carries signals from only one device to another.

Question 13

Refer to the exhibit. What is the maximum possible throughput between the PC and the server?



- 10 Mb/s
- 1000 Mb/s
- **128 kb/s**
- 100 Mb/s

Explanation: The maximum throughput between any two nodes on a network is determined by the slowest link between those nodes.

Question 14

Match the description with the media.

wireless	This type of media provides the most mobility options.
coaxial	Traditionally used for television but can now be used in a network to connect the customer location to the wiring of the customer premises.
optical fiber	This type of media is used for high transmission speed and can also transfer data over long distances.
STP	This type of copper media is used in industrial or similar environments where there is a lot of interference.

Question 15

Which two acronyms represent the data link sublayers that Ethernet relies upon to operate? (Choose two.)

- SFD
- **LLC**
- CSMA
- **MAC**
- FCS

Explanation: For Layer 2 functions, Ethernet relies on logical link control (LLC) and MAC sublayers to operate at the data link layer. FCS (Frame Check Sequence) and SFD (Start Frame Delimiter) are fields of the Ethernet frame. CSMA (Carrier Sense Multiple Access) is the technology Ethernet uses to manage shared media access.

Question 16

A network team is comparing topologies for connecting on a shared media. Which physical topology is an example of a hybrid topology for a LAN?

- bus
- **extended star**
- ring
- partial mesh

Explanation: An extended star topology is an example of a hybrid topology as additional switches are interconnected with other star topologies. A partial mesh topology is a common hybrid WAN topology. The bus and ring are not hybrid topology types.

Question 17

What does a router do when it receives a Layer 2 frame over the network medium?

- re-encapsulates the packet into a new frame
- forwards the new frame appropriate to the medium of that segment of the physical network
- determines the best path
- **de-encapsulates the frame**

Explanation: Routers are responsible for encapsulating a frame with the proper format for the physical network media they connect. At each hop along the path, a router does the following:
Accepts a frame from a medium
De-encapsulates the frame
Determines the best path to forward the packet
Re-encapsulates the packet into a new frame
Forwards the new frame appropriate to the medium of that segment of the physical network

Question 18

Although CSMA/CD is still a feature of Ethernet, why is it no longer necessary?

- the development of half-duplex switch operation
- the use of Gigabit Ethernet speeds
- the use of CSMA/CA

- the virtually unlimited availability of IPv6 addresses
- **the use of full-duplex capable Layer 2 switches**

Explanation: The use of Layer 2 switches operating in full-duplex mode eliminates collisions, thereby eliminating the need for CSMA/CD.

Question 19

What routing table entry has a next hop address associated with a destination network?

- **remote routes**
- directly-connected routes
- local routes
- C and L source routes

Explanation: Routing table entries for remote routes will have a next hop IP address. The next hop IP address is the address of the router interface of the next device to be used to reach the destination network. Directly-connected and local routes have no next hop, because they do not require going through another router to be reached.

Question 20

If the default gateway is configured incorrectly on the host, what is the impact on communications?

- The host is unable to communicate on the local network.
- **The host can communicate with other hosts on the local network, but is unable to communicate with hosts on remote networks.**
- The host can communicate with other hosts on remote networks, but is unable to communicate with hosts on the local network.
- There is no impact on communications.

Explanation: A default gateway is only required to communicate with devices onanother network. The absence of a default gateway does not affect connectivity between devices on the same local network

Question 21

Which term describes a field in the IPv4 packet header that contains a unicast, multicast, or broadcast address?

- **destination IPv4 address**
- protocol
- TTL
- header checksum

Question 22

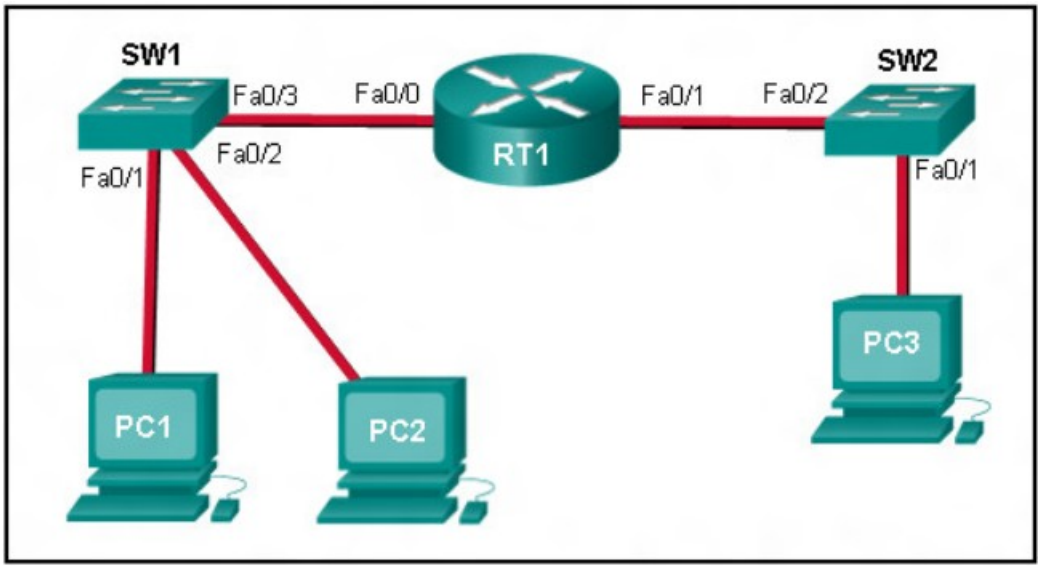
Why is NAT not needed in IPv6?

- Because IPv6 has integrated security, there is no need to hide the IPv6 addresses of internal networks.
- **Any host or user can get a public IPv6 network address because the number of available IPv6 addresses is extremely large.**
- The problems that are induced by NAT applications are solved because the IPv6 header improves packet handling by intermediate routers.
- The end-to-end connectivity problems that are caused by NAT are solved because the number of routes increases with the number of nodes that are connected to the Internet.

Explanation: The large number of public IPv6 addresses eliminates the need for NAT. Sites from the largest enterprises to single households can get public IPv6 network addresses. This avoids some of the NAT-induced application problems that are experienced by applications that require end-to-end connectivity.

Question 23

Refer to the exhibit. PC1 issues an ARP request because it needs to send a packet to PC3. In this scenario, what will happen next?



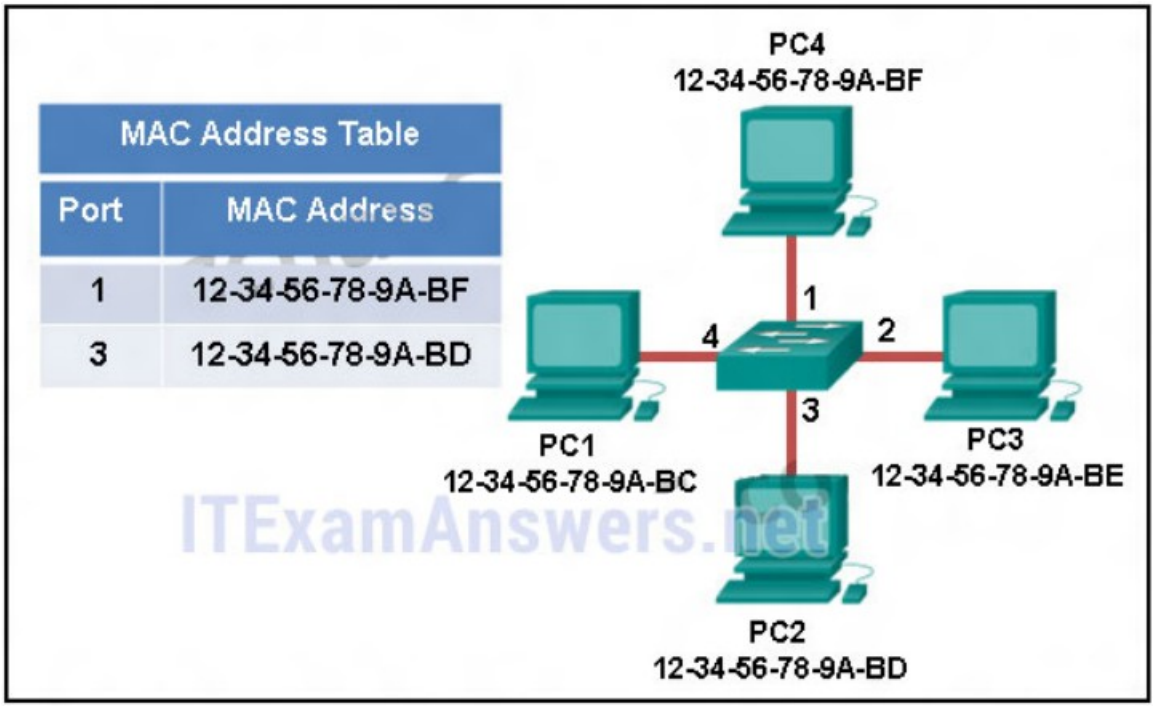
- RT1 will send an ARP reply with its own Fa0/1 MAC address.
- SW1 will send an ARP reply with its Fa0/1 MAC address.
- RT1 will send an ARP reply with the PC3 MAC address.
- RT1 will forward the ARP request to PC3.
- **RT1 will send an ARP reply with its own Fa0/0 MAC address.**

Explanation: When a network device has to communicate with a device on another network, it broadcasts an ARP request asking for the default gateway MAC address. The default gateway (RT1) unicasts an ARP reply with the Fa0/0 MAC address.

Question 24

Refer to the exhibit. The exhibit shows a small switched network and the contents of the MAC address table of the switch. PC1 has sent a frame addressed to PC3. What will the

switch do with the frame?



- The switch will discard the frame.
- The switch will forward the frame only to port 2.
- **The switch will forward the frame to all ports except port 4.**
- The switch will forward the frame to all ports.
- The switch will forward the frame only to ports 1 and 3.

Explanation: The MAC address of PC3 is not present in the MAC table of the switch. Because the switch does not know where to send the frame that is addressed to PC3, it will forward the frame to all the switch ports, except for port 4, which is the incoming port.

Question 25

Which destination address is used in an ARP request frame?

- 0.0.0.0
- 255.255.255.255
- **FFFF.FFFF.FFFF**
- AAAA.AAAA.AAAA
- the physical address of the destination host

Explanation: The purpose of an ARP request is to find the MAC address of the destination host on an Ethernet LAN. The ARP process sends a Layer 2 broadcast to all devices on the Ethernet LAN. The

frame contains the IP address of the destination and the broadcast MAC address, FFFF.FFFF.FFFF. The host with the IP address that matches the IP address in the ARP request will reply with a unicast frame that includes the MAC address of the host. Thus the original sending host will obtain the destination IP and MAC address pair to continue the encapsulation process for data transmission.

Question 26

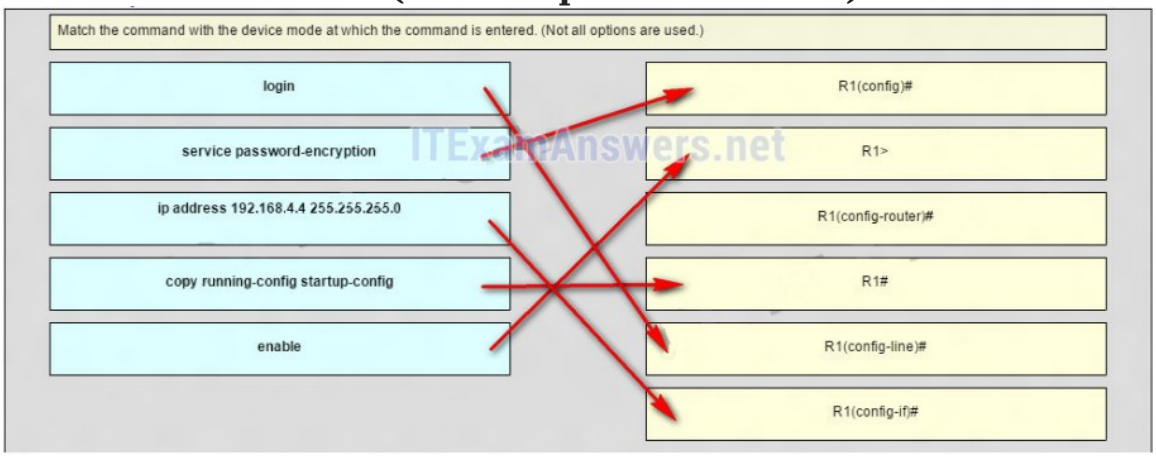
A router boots and enters setup mode. What is the reason for this?

- The IOS image is corrupt.
- Cisco IOS is missing from flash memory.
- **The configuration file is missing from NVRAM.**
- The POST process has detected hardware failure.

Explanation: If a router cannot locate the startup-config file in NVRAM it will enter setup mode to allow the configuration to be entered from the console device.

Question 27

Match the command with the device mode at which the command is entered. (Not all options are used.)



Explanation:
The **enable** command is entered **in R1>** mode.
The **login** command is entered in **R1(config-line)#** mode.
The **copy running-config startup-config** command is entered in **R1#** mode.

The **ip address 192.168.4.4 255.255.255.0** command is entered in **R1(config-if)#** mode.
The **service password-encryption** command is entered in **R1(config)#** mode (global configuration mode).

Question 28

```
Floor(config)# interface gi0/1
Floor(config-if)# description Connects to the Registrar LAN
Floor(config-if)# ip address 192.168.235.234 255.255.255.0
Floor(config-if)# no shutdown
Floor(config-if)# interface gi0/0
Floor(config-if)# description Connects to the Manager LAN
Floor(config-if)# ip address 192.168.234.114 255.255.255.0
Floor(config-if)# no shutdown
Floor(config-if)# interface s0/0/0
Floor(config-if)# description Connects to the ISP
Floor(config-if)# ip address 10.234.235.254 255.255.255.0
Floor(config-if)# no shutdown
Floor(config-if)# interface s0/0/1
Floor(config-if)# description Connects to the Head Office WAN
Floor(config-if)# ip address 203.0.113.3 255.255.255.0
Floor(config-if)# no shutdown
Floor(config-if)# end
```

Refer to the exhibit. A network administrator is connecting a new host to the Registrar LAN. The host needs to communicate with remote networks. What IP address would be configured as the default gateway on the new host?

- **192.168.235.234**
- 192.168.235.1
- 10.234.235.254
- 203.0.113.3
- 192.168.234.114

Question 29

What type of address is 198.133.219.162?

- link-local
- **public**
- loopback
- multicast

Question 30

What does the IP address 192.168.1.15/29 represent?

- multicast address
- **broadcast address**
- unicast address
- subnetwork address

Explanation: A broadcast address is the last address of any given network. This address cannot be assigned to a host, and it is used to communicate with all hosts on that network.

Question 31

Three devices are on three different subnets. Match the network address and the broadcast address with each subnet where these devices are located. (Not all options are used.)

Device 1: IP address 192.168.10.77/28 on subnet 1

Device 2: IP address192.168.10.17/30 on subnet 2

Device 3: IP address 192.168.10.35/29 on subnet 3

Place the options in the following order:

Subnet 2 network number	192.168.10.16
Subnet 1 broadcast address	192.168.10.79
Subnet 3 broadcast address	192.168.10.39
Subnet 2 broadcast address	192.168.10.19
Subnet 1 network number	192.168.10.64
Subnet 3 network number	192.168.10.32

Explanation: To calculate any of these addresses, write the device IP address in binary. Draw a line showing where the subnet mask 1s end. For example, with Device 1, the final octet (77) is 01001101. The line would be drawn between the 0100 and the 1101 because the subnet mask is /28. Change all the bits to the right of the line to 0s to determine the network number (01000000 or 64). Change all the bits to the right of the line to 1s to determine the broadcast address (01001111 or 79).

Question 32

Given network 172.18.109.0, which subnet mask would be used if 6 host bits were available?

- 255.255.192.0
- 255.255.224.0
- **255.255.255.192**
- 255.255.255.248
- 255.255.255.252

Explanation:
With an IPv4 network, the subnet mask is determined by the hosts bits that are required:
11 host bits required – 255.255.248.0
10 host bits required – 255.255.252.0
9 host bits required – 255.255.254.0
8 host bits required – 255.255.255.0
7 host bits required – 255.255.255.128
6 host bits required – 255.255.255.192
5 host bits required – 255.255.255.224
4 host bits required – 255.255.255.240
3 host bits required – 255.255.255.248
2 host bits required – 255.255.255.252

Question 33

Which is the compressed format of the IPv6 address fe80:0000:0000:0000:0220:0b3f:f0e0:0029?

- **fe80::220:b3f:f0e0:29**
- fe80:9ea:0:2200::fe0:290
- fe80:9ea0::2020:0:bf:e0:9290
- fe80:9ea0::2020::bf:e0:9290

Question 34

```
C:\Windows\system32> netstat -r
<output omitted>

IPv6 Route Table
===========================================================
Active Routes:
 If Metric Network Destination      Gateway
  9    306 ::/0                     On-link
  1    306 ::1/128                  On-link
  9    306 2001::/32                On-link
  9    306 2001:0:9d38:6ab8:30d0:115:3f57:fe4c/128
                                    On-link
  4    281 fe80::/64                On-link
  9    306 fe80::/64                On-link
  4    281 fe80::1c20:5d8b:4b44:bd40/128
                                    On-link
  9    306 fe80::30d0:115:3f57:fe4c/128
                                    On-link
  1    306 ff00::/8                 On-link
  4    281 ff00::/8                 On-link
  9    306 ff00::/8                 On-link
===========================================================
```

ITExamAnswers.net

Refer to the exhibit. A user issues the command netstat –r on a workstation. Which IPv6 address is one of the link-local addresses of the workstation?

- ::1/128
- **fe80::30d0:115:3f57:fe4c/128**
- fe80::/64
- 2001:0:9d38:6ab8:30d0:115:3f57:fe4c/128

Explanation: In the IPv6 address scheme, the network of fe80::/10 is reserved for link-local addresses. The address fe80::/64 is a network address that indicates, in this workstation, fe80::/64 is actually used for link-local addresses. Thus the address fe80::30d0:115:3f57:fe4c/128 is a valid IPv6 link-local address.

Question 35

What type of IPv6 address is represented by ::1/128?

- EUI-64 generated link-local
- global unicast
- unspecified
- **loopback**

Question 36

Which two ICMP messages are used by both IPv4 and IPv6 protocols? (Choose two.)?

- router solicitation
- **route redirection**
- neighbor solicitation
- **protocol unreachable**
- router advertisement

Explanation: The ICMP messages common to both ICMPv4 and ICMPv6 include: host confirmation, destination (net, host, protocol, port) or service unreachable, time exceeded, and route redirection. Router solicitation, neighbor solicitation, and router advertisement are new protocols implemented in ICMPv6.

Question 37

A Wireshark capture is shown with the Transmission Control Protocol section expanded. The item highlighted states Window size: 9017.

- tracing the path to a host computer on the network and the network has the IP address 127.0.0.1
- **testing the integrity of the TCP/IP stack on the local machine**
- pinging a host computer that has the IP address 127.0.0.1 on the network
- checking the IP address on the network card

Explanation: 127.0.0.1 is an address reserved by TCP/IP to test the NIC, drivers and TCP/IP implementation of the device.

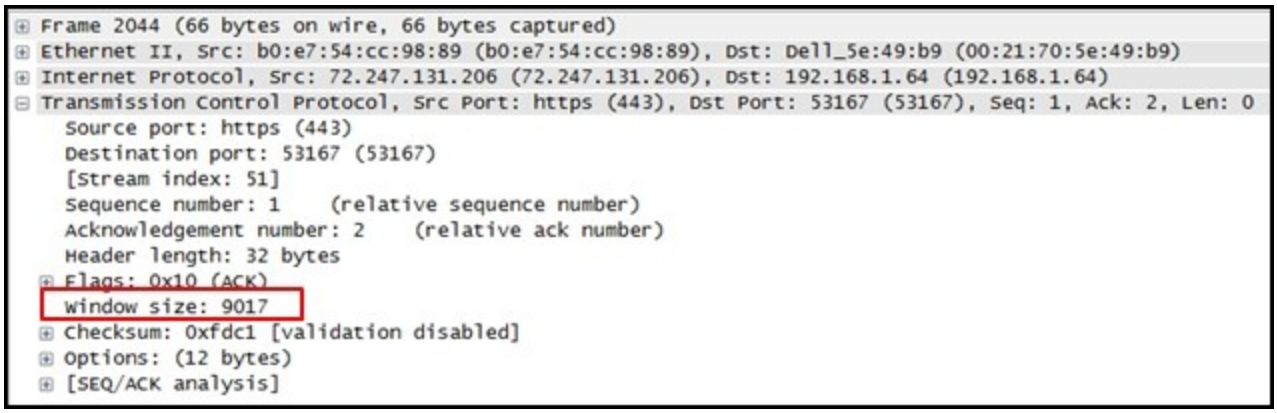
Question 38

24. Network information:
* local router LAN interface: 172.19.29.254 / fe80:65ab:dcc1::10
* local router WAN interface: 198.133.219.33 / 2001:db8:FACE:39::10
* remote server: 192.135.250.103

What task might a user be trying to accomplish by using the ping 2001:db8:FACE:39::10 command?

- verifying that there is connectivity within the local network
- creating a network performance benchmark to a server on the company intranet
- determining the path to reach the remote server
- **verifying that there is connectivity to the internet**

Question 39


Frame 2044 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: b0:e7:54:cc:98:89 (b0:e7:54:cc:98:89), Dst: Dell_5e:49:b9 (00:21:70:5e:49:b9)
Internet Protocol, Src: 72.247.131.206 (72.247.131.206), Dst: 192.168.1.64 (192.168.1.64)
Transmission Control Protocol, Src Port: https (443), Dst Port: 53167 (53167), Seq: 1, Ack: 2, Len: 0
Source port: https (443)
Destination port: 53167 (53167)
[Stream index: 51]
Sequence number: 1 (relative sequence number)
Acknowledgement number: 2 (relative ack number)
Header length: 32 bytes
Flags: 0x10 (ACK)
Window size: 9017
Checksum: 0xfdc1 [validation disabled]
Options: (12 bytes)
[SEQ/ACK analysis]

Refer to the exhibit. What does the value of the window size specify?

- the amount of data that can be sent at one time
- **the amount of data that can be sent before an acknowledgment is required**
- the total number of bits received during this TCP session
- a random number that is used in establishing a connection with the 3-way handshake

Explanation: The window size determines the number of bytes that can be sent before expecting an acknowledgment. The acknowledgment number is the number of the next expected byte.

Question 40

To which TCP port group does the port 414 belong?

- **well-known**
- private or dynamic
- public
- registered

Explanation:

Well Known Ports: 0 through 1023.
Registered Ports: 1024 through 49151.
Dynamic/Private : 49152 through 65535.

Question 41

A client packet is received by a server. The packet has a destination port number of 22. What service is the client requesting?

- **SSH**
- SMB/CIFS
- HTTPS
- SLP

Question 42

Two students are working on a network design project. One student is doing the drawing, while the other student is writing the proposal. The drawing is finished and the student wants to share the folder that contains the drawing so that the other student can access the file and copy it to a USB drive. Which networking model is being used?

- **peer-to-peer**
- client-based
- master-slave
- point-to-point

Explanation: In a peer-to-peer (P2P) networking model, data is exchanged between two network devices without the use of a dedicated server.

Question 43

What service is provided by POP3?

- **Retrieves email from the server by downloading the email to the local mail application of the client.**
- An application that allows real-time chatting among remote users.
- Allows remote access to network devices and servers.

- Uses encryption to provide secure remote access to network devices and servers.

Question 44

Which command is used to manually query a DNS server to resolve a specific hostname?

- net
- tracert
- **nslookup**
- ipconfig /displaydns

Explanation: The nslookup command was created to allow a user to manually query a DNS server to resolve a given host name. The ipconfig /displaydns command only displays previously resolved DNS entries. The tracert command was created to examine the path that packets take as they cross a network and can resolve a hostname by automatically querying a DNS server. The net command is used to manage network computers, servers, printers, and network drives.

Question 45

The employees and residents of Ciscoville cannot access the Internet or any remote web-based services. IT workers quickly determine that the city firewall is being flooded with so much traffic that a breakdown of connectivity to the Internet is occurring. Which type of attack is being launched at Ciscoville?

- access
- Trojan horse
- reconnaissance
- **DoS**

Explanation: A DoS (denial of service) attack prevents authorized users from using one or more computing resources.

Question 46

Which statement describes the characteristics of packet-filtering and stateful firewalls as they relate to the OSI model?

- A packet-filtering firewall uses session layer information to track the state of a connection, whereas a stateful firewall uses application layer information to track the state of a connection.
- Both stateful and packet-filtering firewalls can filter at the application layer.
- **A packet-filtering firewall typically can filter up to the transport layer, whereas a stateful firewall can filter up to the session layer.**
- A stateful firewall can filter application layer information, whereas a packet-filtering firewall cannot filter beyond the network layer.

Explanation: Packet filtering firewalls can always filter Layer 3 content and sometimes TCP and UDP-based content. Stateful firewalls monitor connections and thus have to be able to support up to the session layer of the OSI model.

Question 47

What are two ways to protect a computer from malware? (Choose two.)

- Empty the browser cache.
- **Use antivirus software.**
- Delete unused software.
- **Keep software up to date.**
- Defragment the hard disk.

Explanation: At a minimum, a computer should use antivirus software and have all software up to date to defend against malware.

Question 48

A network administrator is issuing the login block-for 180 attempts 2 within 30 command on a router. Which threat is the network administrator trying to prevent?

- **a user who is trying to guess a password to access the router**
- a worm that is attempting to access another part of the network
- an unidentified individual who is trying to access the network equipment room
- a device that is trying to inspect the traffic on a link

Explanation: The login block-for 180 attempts 2 within 30 command will cause the device to block authentication after 2 unsuccessful attempts within 30 seconds for a duration of 180 seconds. A device inspecting the traffic on a link has nothing to do with the router. The router configuration cannot prevent unauthorized access to the equipment room. A worm would not attempt to access the router to propagate to another part of the network.

Question 49

Which two commands could be used to check if DNS name resolution is working properly on a Windows PC? (Choose two.)

- **nslookup cisco.com**
- net cisco.com
- ipconfig /flushdns
- nbtstat cisco.com
- **ping cisco.com**

Explanation: The **ping** command tests the connection between two hosts. When ping uses a host domain name to test the connection, the resolver on the PC will first perform the name resolution to query the DNS server for the IP address of the host. If the ping command is unable to resolve the domain name to an IP address, an error will result.
Nslookup is a tool for testing and troubleshooting DNS servers.

Question 50

A small advertising company has a web server that provides critical business service. The company connects to the Internet through a leased line service to an ISP. Which approach best provides cost effective redundancy for the Internet connection?

- Add a second NIC to the web server.
- **Add a connection to the Internet via a DSL line to another ISP.**
- Add another web server to prepare failover support.
- Add multiple connections between the switches and the edge router.

Explanation: With a separate DSL connection to another ISP, the company will have a redundancy solution for the Internet connection,

in case the leased line connection fails. The other options provide other aspects of redundancy, but not the Internet connection. The options of adding a second NIC and adding multiple connections between the switches and the edge router will provide redundancy in case one NIC fails or one connection between the switches and the edge router fails. The option of adding another web server provides redundancy if the main web server fails.

Question 51

Only employees connected to IPv6 interfaces are having difficulty connecting to remote networks. The analyst wants to verify that IPv6 routing has been enabled. What is the best command to use to accomplish the task?

- **show running-config**
- show interfaces
- copy running-config startup-config
- show ip nat translations

Question 52

Two network engineers are discussing the methods used to forward frames through a switch. What is an important concept related to the cut-through method of switching?

- The fragment-free switching offers the lowest level of latency.
- Fast-forward switching can be viewed as a compromise between store-and-forward switching and fragment-free switching.
- Fragment-free switching is the typical cut-through method of switching.
- **Packets can be relayed with errors when fast-forward switching is used.**

Explanation: Fast-forward switching offers the lowest level of latency and it is the typical cut-through method of switching. Fragment-free switching can be viewed as a compromise between store-and-forward switching and fast-forward switching. Because fast-forward switching starts forwarding before the entire packet has been received, there may be times when packets are relayed with errors.

Question 53

What happens when a switch receives a frame and the calculated CRC value is different than the value that is in the FCS field?

- The switch notifies the source of the bad frame.
- The switch places the new CRC value in the FCS field and forwards the frame.
- **The switch drops the frame.**
- The switch floods the frame to all ports except the port through which the frame arrived to notify the hosts of the error.

Explanation: The purpose of the CRC value in the FCS field is to determine if the frame has errors. If the frame does have errors, then the frame is dropped by the switch.

Question 54

Which two functions are performed at the LLC sublayer of the OSI Data Link Layer to facilitate Ethernet communication? (Choose two.)

- implements CSMA/CD over legacy shared half-duplex media
- **enables IPv4 and IPv6 to utilize the same physical medium**
- integrates Layer 2 flows between 10 Gigabit Ethernet over fiber and 1 Gigabit Ethernet over copper
- implements a process to delimit fields within an Ethernet 2 frame
- **places information in the Ethernet frame that identifies which network layer protocol is being encapsulated by the frame**

Other case

- responsible for internal structure of Ethernet frame
- applies source and destination MAC addresses to Ethernet frame
- integrates Layer 2 flows between 10 Gigabit Ethernet over fiber and 1 Gigabit Ethernet over copper
- **enables IPv4 and IPv6 to utilize the same physical medium**
- **handles communication between upper layer networking software and Ethernet NIC hardware**

Other case

- **adds Ethernet control information to network protocol data**
- responsible for internal structure of Ethernet frame
- implements trailer with frame check sequence for error detection
- **enables IPv4 and IPv6 to utilize the same physical medium**
- applies source and destination MAC addresses to Ethernet frame

Other case

- implements CSMA/CD over legacy shared half-duplex media
- **adds Ethernet control information to network protocol data**
- **places information in the Ethernet frame that identifies which network layer protocol is being encapsulated by the frame**
- applies source and destination MAC addresses to Ethernet frame
- integrates Layer 2 flows between 10 Gigabit Ethernet over fiber and 1 Gigabit Ethernet over copper

Explanation: The data link layer is actually divided into two sublayers:
+ Logical Link Control (LLC): This upper sublayer defines the software processes that provide services to the network layer protocols. It places information in the frame that identifies which network layer protocol is being used for the frame. This information allows multiple Layer 3 protocols, such as IPv4 and IPv6, to utilize the same network interface and media.
+ Media Access Control (MAC): This lower sublayer defines the media access processes performed by the hardware. It provides data link layer addressing and delimiting of data according to the physical signaling requirements of the medium and the type of data link layer protocol in use.

Question 55

Which two issues can cause both runts and giants in Ethernet networks? (Choose two.)

- **a malfunctioning NIC**
- CRC errors
- electrical interference on serial interfaces

- **half-duplex operations**
- using the incorrect cable type

Explanation: Because collisions are a normal aspect of half-duplex communications, runt and giant frames are common by-products of those operations. A malfunctioning NIC can also place frames on the network that are either too short or longer than the maximum allowed length. CRC errors can result from using the wrong type of cable or from electrical interference. Using a cable that is too long can result in late collisions rather than runts and giants.

100%

You have scored 100%.

Congratulations, you have passed the exam.

You have used 1 of 1 attempt(s).

Review Assessment

Here is how you performed in each of the Learning Objectives and Skills associated with this assessment.

Network Basics. Connectivity	100%
Basic Device Management. Initial Device Config	100%
Network Basics. Protocols	100%
IP Addressing. IPv4	100%
Security. Security Fundamentals	100%
Network Basics. Communications	100%
Network Basics. Ethernet	100%
IP Addressing. IPv6	100%
Network Basics. Network Fundamentals	100%